CONFIDENTIALITY POLICY

Version 2/2026 VNG-GOV-CONF-PL-02

Effective Date: 10 August 2026

VANACHAI GROUP

Confidentiality Policy
Vanachai Group Public Company Limited and Subsidiaries

Vanachai Group Public Company Limited and its subsidiaries (the "Company") recognize that confidential information, business information, personal data, technical knowledge, intellectual property, trade secrets, financial information, customer and supplier information, employee information, commercial terms, strategic plans, production information and digital records are critical assets that support competitiveness, trust, governance, innovation and long-term value creation.

The Company is committed to protecting confidential information against unauthorized access, use, disclosure, copying, loss, alteration, destruction, leakage or misuse, whether such information is held in physical, electronic, verbal, visual or cloud-based form. The Company also recognizes that inappropriate disclosure of confidential information may cause legal, financial, operational, reputational and stakeholder impacts.

This Policy establishes the principles, governance structure, responsibilities and control measures for identifying, classifying, protecting, using, storing, sharing, retaining and disposing of confidential information. It supports the Company's governance, risk management, internal control, data privacy, information technology security and responsible business conduct frameworks.

This policy is approved and issued for acknowledgement and implementation by all relevant parties.

1) Objectives

- Establish a clear corporate framework for protecting confidential information and preventing unauthorized disclosure or misuse.
- Ensure that directors, executives, employees and relevant third parties understand their responsibilities in handling confidential information.
- Protect the Company's commercial interests, competitiveness, reputation, intellectual property, personal data, trade secrets and stakeholder trust.
- Ensure that confidential information is accessed and disclosed only for lawful, authorized and legitimate business purposes under the need-to-know principle.
- Promote compliance with applicable laws, regulations, contracts, non-disclosure obligations, corporate governance principles and internal policies.
- Strengthen controls over data classification, access management, secure storage, secure communication, retention, disposal, incident reporting and third-party confidentiality obligations.

- Integrate confidentiality risk management into the Company's Enterprise Risk Management framework and daily business operations.

2) Policy Alignment and International Standards

- Thailand Personal Data Protection Act B.E. 2562 and related subordinate regulations, where personal data is involved.
- Thailand Trade Secrets Act B.E. 2545 and related intellectual property laws, where confidential business information, technical information or commercial information qualifies as a trade secret or intellectual property.
- Computer Crime Act B.E. 2550 and amendments, Cybersecurity Act B.E. 2562, Electronic Transactions Act and other applicable laws relating to information systems, electronic records and digital communication.
- Securities and Exchange Act, SEC and SET corporate governance expectations, where confidential information may include material non-public information or market-sensitive information.
- ISO/IEC 27001 Information Security Management Systems, ISO/IEC 27002 Information Security Controls and ISO/IEC 27701 Privacy Information Management, where applicable to the Company's context and maturity.
- NIST Cybersecurity Framework principles on governance, identification, protection, detection, response and recovery, where applicable.
- GRI Standards: GRI 2-23 Policy Commitments, GRI 2-24 Embedding Policy Commitments, GRI 2-27 Compliance with Laws and Regulations, GRI 3-3 Management of Material Topics and GRI 418 Customer Privacy, where applicable.
- FTSE Russell ESG Indicators relating to corporate governance, risk management, cybersecurity, data privacy, business ethics, internal controls and supply chain governance, where applicable.
- The Company's Code of Conduct, Information Technology Security Policy, Personal Data Protection and Privacy Notice, Prevention of the Use of Inside Information for Personal Gain Policy, Whistleblowing Policy, Human Rights Policy, procurement requirements and other relevant internal procedures.

3) Scope of the Policy

This policy applies to:

- This policy applies to the Company, its subsidiaries and joint ventures under the Company's operational control.
- This policy applies to directors, executives, employees, temporary staff, interns, contractors, consultants, outsourced personnel and any person who has access to the Company's confidential information.

- This policy applies to suppliers, customers, agents, service providers, cloud service providers, software vendors, auditors, advisors, consultants and business partners who receive, process, store, transmit or manage confidential information of the Company.
- This policy covers all confidential information in all forms, including paper documents, electronic files, emails, databases, system records, images, drawings, product formulas, technical information, business plans, financial information, commercial terms, meeting materials, verbal communications, cloud records and information stored on devices.
- This policy applies throughout the information life cycle, including creation, collection, classification, access, use, disclosure, transmission, storage, retention, archiving, return, disposal and destruction.

4) Definitions and References

To ensure a consistent understanding and application of this Confidentiality Policy, the following key terms are defined as follows.

- **Confidential Information:** Any non-public information that belongs to, is controlled by, is entrusted to or is used by the Company and that may cause harm or disadvantage to the Company or stakeholders if disclosed without authorization.
- **Restricted Information:** Highly sensitive confidential information that requires stricter protection due to legal, strategic, financial, commercial, personal data, trade secret or market-sensitive implications.
- **Internal Information:** Information intended for internal business use within the Company and not for public disclosure unless authorized.
- **Public Information:** Information that has been formally approved for public disclosure through authorized channels.
- **Personal Data:** Information relating to an identifiable person, as defined by applicable personal data protection laws.
- **Trade Secret:** Business, technical or commercial information that is not generally known, has commercial value because it is confidential and is subject to reasonable measures to keep it confidential.
- **Material Non-Public Information:** Non-public information that may reasonably affect securities prices, investor decisions, business valuation or stakeholder decisions, and must be handled in accordance with the Company's inside information policy.
- **Data Owner:** A department, function or authorized person responsible for determining the classification, access rights, use, retention and disposal of information.

- **Data Custodian:** A person or function responsible for maintaining, storing, securing or operating systems that hold confidential information.
- **Need-to-Know Principle:** Access to confidential information shall be limited to persons who require such information to perform authorized duties or fulfill legitimate business purposes.
- **Non-Disclosure Agreement (NDA):** A written agreement requiring a person or organization to protect confidential information and restrict its use and disclosure.
- **Information Leakage:** Unauthorized disclosure, transfer, loss or exposure of confidential information, whether intentional, accidental or caused by negligence.
- **Vanachai Integrated Materiality and Risk Assessment (V-IMRA):** The Company's internal process for identifying and prioritizing sustainability, governance and business risks by integrating impact and financial materiality perspectives to support enterprise risk management, strategic planning and decision-making.

5) Governance and Accountability

- **Board of Directors:** Approves this policy and oversees the Company's governance, risk management, internal control and ethical conduct relating to confidentiality and information protection.
- **Risk Management and Governance Committee:** Oversees confidentiality-related risks, including data leakage, improper disclosure, conflicts of interest, information misuse, third-party data risks and integration into the Enterprise Risk Management framework.
- **Audit Committee:** Reviews the adequacy and effectiveness of internal controls, audit findings and corrective actions relating to confidentiality, access control and information protection.
- **Managing Director and Management:** Ensure that resources, systems, procedures, training and enforcement mechanisms are provided for effective implementation of this policy.
- **Legal, Compliance and Company Secretary Functions:** Provide guidance on legal obligations, contractual confidentiality clauses, non-disclosure arrangements, regulatory disclosures and market-sensitive information.
- **Information Technology Department:** Implements and maintains technical controls to protect confidential information, including access control, authentication, encryption, logging, backup, cloud security and incident response.
- **Human Resources Department:** Embeds confidentiality obligations into employment processes, onboarding, training, disciplinary procedures, transfers, resignations and exit processes.

- **Department Heads and Data Owners:** Classify information, approve access rights, ensure appropriate use and disclosure and monitor compliance within their areas of responsibility.
- **Internal Audit:** Conducts independent reviews of confidentiality controls and reports findings to relevant governance bodies.
- **Employees and Relevant Third Parties:** Comply with this policy, protect confidential information, use information only for authorized purposes and promptly report suspected breaches or information leakage.

6) Commitments and Principles

6.1 Legal Compliance and Ethical Conduct

- Comply with applicable laws, regulations, contractual obligations, non-disclosure obligations and internal policies relating to confidential information, personal data, trade secrets, intellectual property and market-sensitive information.
- Use confidential information only for legitimate business purposes and in a manner consistent with honesty, integrity and professional responsibility.

6.2 Information Classification and Need-to-Know Access

- Classify information according to sensitivity, business importance, legal requirements and potential impact from unauthorized disclosure.
- Limit access to confidential information under the need-to-know and least-privilege principles, with appropriate approval and periodic review.

6.3 Protection, Use and Disclosure Controls

- Protect confidential information from unauthorized access, copying, modification, transfer, disclosure, destruction, loss or misuse.
- Disclose confidential information only to authorized persons or organizations, and only when necessary for approved business purposes or legal requirements.

6.4 Secure Storage, Transmission and Communication

- Store confidential information in approved systems, secured physical locations or controlled digital repositories with appropriate access controls.
- Use secure communication channels, encryption or other protective measures when transmitting restricted or sensitive information.

6.5 Personal Data and Privacy Protection

- Handle personal data in accordance with applicable privacy laws, the Company's privacy notices and data protection procedures.
- Collect, use, disclose, retain and delete personal data only to the extent necessary for lawful and specified purposes.

6.6 Trade Secrets, Intellectual Property and Business Know-How

- Protect product development information, formulas, technical knowledge, production processes, customer insights, commercial strategies, research and innovation information as confidential assets.
- Prevent unauthorized disclosure or use of trade secrets and intellectual property belonging to the Company, customers, suppliers or business partners.

6.7 Inside Information and External Communication

- Handle material non-public information in accordance with the Company's policy on prevention of the use of inside information for personal gain.
- Ensure that external communication, media statements, investor communication, public reports and regulatory disclosures are made only by authorized persons through approved channels.

6.8 Third-Party Confidentiality

- Require appropriate confidentiality clauses, non-disclosure agreements, data protection agreements or equivalent safeguards before sharing confidential information with third parties.
- Ensure that third parties receiving confidential information use it only for the agreed purpose and apply appropriate security controls.

6.9 Retention, Return and Secure Disposal

- Retain confidential information only for the period required by law, contract or business necessity.
- Return, delete, destroy or archive confidential information securely when it is no longer required or when an employment, contract or business relationship ends.

6.10 Incident Reporting and Accountability

- Report suspected or actual loss, leakage, unauthorized disclosure or misuse of confidential information immediately through the designated reporting channels.
- Apply corrective actions, disciplinary measures and legal remedies where breaches of confidentiality occur.

7) Risk, Impact, and Dependency Management

- The risks, impacts and dependencies associated with the matters addressed in this policy are identified, analyzed and prioritized through the Company's Vanachai Integrated Materiality and Risk Assessment (V-IMRA) process. V-IMRA considers both impact materiality and financial materiality across the value chain.
- The results of V-IMRA are integrated into the Enterprise Risk Management (ERM) system to support policy formulation, strategic decision-making, internal control, risk appetite, risk ownership and long-term value creation.

- Key confidentiality risks include unauthorized disclosure, information leakage, improper access, cyber intrusion, insider misuse, loss of documents or devices, third-party data exposure, inappropriate public communication, employee turnover, social engineering, cloud misconfiguration and use of unapproved digital tools.
- The Company shall assess confidentiality risks by considering information sensitivity, legal obligations, business criticality, stakeholder impact, potential financial loss, reputational harm and likelihood of occurrence.
- Risk responses shall include information classification, access control, non-disclosure agreements, secure communication, encryption, clean desk and clear screen practices, user awareness, secure disposal, monitoring, incident response and corrective action.
- Material confidentiality incidents and control weaknesses shall be reported to relevant management and governance bodies, with follow-up until corrective actions are completed.

8) Targets and Metrics

- Percentage of employees and relevant users completing confidentiality, data privacy and information security awareness training.
- Percentage of critical confidential information repositories with assigned data owners and approved access controls.
- Percentage of user access rights for sensitive systems reviewed at least annually or upon role change, transfer, resignation or contract termination.
- Percentage of relevant contracts with suppliers, contractors, consultants and business partners containing confidentiality or non-disclosure clauses.
- Number and severity of confidentiality breaches, information leakage incidents, unauthorized access events and personal data incidents.
- Average time to acknowledge, contain, investigate and close confidentiality-related incidents.
- Percentage of critical third parties assessed for confidentiality, data privacy and information security controls where applicable.
- Number of corrective actions from audits, incidents or reviews completed within the defined timeframe.
- Annual reporting of confidentiality performance, major risks and improvement actions to relevant governance bodies.

9) Supply Chain and Partner Responsibility

- Require suppliers, contractors, consultants, advisors, cloud providers, software vendors and business partners to protect confidential information received from the Company.

- Include confidentiality, non-disclosure, data protection, access control, incident notification, audit rights, subcontracting and return or destruction requirements in relevant contracts and purchase documents.
- Conduct confidentiality and information security due diligence for critical third parties based on the sensitivity of information and criticality of services.
- Limit third-party access to confidential information to approved, documented, time-bound and need-to-know purposes, with prompt revocation when access is no longer required.
- Require third parties to ensure that their employees, subcontractors and agents who access the Company's confidential information are bound by equivalent confidentiality obligations.
- Ensure that confidential information is returned, deleted or securely destroyed upon contract completion, service termination or request by the Company, subject to legal and contractual retention requirements.

10) Integration with Corporate Strategy

This policy supports the Company's corporate governance, risk management, digital transformation, innovation, customer trust, supplier collaboration, sustainability reporting and business continuity objectives.

- **FOREST:** Protect sourcing, traceability, plantation, production, environmental and sustainability-related information that supports responsible management of natural resources and wood-based products.
- **FUTURE**: Protect innovation, research and development, product design, digital systems, commercial strategy and business intelligence to strengthen long-term competitiveness.
- **TOGETHER:** Strengthen stakeholder trust by protecting employee, customer, supplier, community, investor and business partner information through responsible and transparent information governance.

Integrate confidentiality considerations into procurement, contract management, employee lifecycle management, project management, product development, digital transformation, external communication and disclosure processes.

11) Implementation and Management Tools

11.1 Information Classification and Labelling

- Establish practical classification levels such as Public, Internal, Confidential and Restricted, with appropriate handling requirements for each level.
- Label confidential documents, electronic files, presentations and emails where appropriate to indicate sensitivity and handling requirements.

11.2 Access Control and Authorization

- Apply approval workflows, role-based access, least privilege, authentication, access logs and periodic access review for confidential information and sensitive systems.
- Revoke access promptly when employees transfer, resign, terminate employment or no longer require access for their duties.

11.3 Contractual and Legal Tools

- Use confidentiality clauses, non-disclosure agreements, data processing agreements and intellectual property clauses as appropriate for employees, suppliers, contractors, consultants and business partners.
- Review contractual obligations before sharing confidential information with external parties.

11.4 Secure Work Practices

- Apply clean desk and clear screen practices, secure printing, controlled meeting materials, secure file sharing, approved communication channels and careful handling of portable devices.
- Avoid discussing confidential matters in public areas or sharing confidential information through unapproved personal email, personal cloud storage, messaging applications or social media.

11.5 Training and Awareness

- Provide orientation and periodic training on confidentiality obligations, data privacy, insider information, phishing awareness, document handling, third-party disclosure and incident reporting.
- Communicate practical examples of prohibited conduct and expected behavior to strengthen the Company's confidentiality culture.

11.6 Incident Response and Remediation

- Maintain reporting channels for suspected or actual confidentiality breaches, including management reporting, whistleblowing channels, IT Service Center or other designated channels.
- Investigate incidents, contain risks, recover information where possible, notify relevant parties where required and implement corrective and preventive actions.

11.7 Record Retention and Secure Disposal

- Maintain retention schedules for confidential information based on legal, contractual and business requirements.
- Dispose of confidential information through approved secure methods, including shredding, secure deletion, degaussing or certified destruction where appropriate.

12) Monitoring, Reporting and Transparency

- Monitor compliance with confidentiality requirements through access reviews, audit activities, incident records, contract reviews, supplier assessments, training completion and management reporting.
- Report significant confidentiality risks, incidents, audit findings and corrective actions to relevant management and governance bodies.
- Maintain records of access approvals, NDAs, confidentiality clauses, third-party disclosures, incident reports, investigation results, training completion and corrective actions.
- Ensure that public disclosure of information through annual reports, sustainability reports, websites, press releases, investor communication and other channels is reviewed and approved by authorized persons before release.
- Disclose only appropriate high-level information on confidentiality governance and risk management, without revealing confidential information or creating additional security or commercial risk.

13) Review and Continuous Improvement

- This policy shall be reviewed at least every two years, or earlier if there are changes in laws, regulations, business operations, information systems, stakeholder expectations, risk profile, audit findings or significant confidentiality incidents.
- The Company shall continuously improve confidentiality controls in alignment with evolving business practices, digital transformation, legal requirements, cybersecurity threats and lessons learned from incidents.
- The policy owner, in coordination with relevant departments, shall prepare policy review results and improvement recommendations for management and governance review.
- Training, access reviews, internal audits, supplier reviews, incident analysis and employee feedback shall be used to strengthen the Company's confidentiality culture and information governance.

14) Confidentiality Policy Revision History

Version	Date	Policy Owner	Approved by	Key Changes / Comments
1.0	11 November 2024	Sustainable Development Task Force	Board of Directors	Initial issue of the Confidentiality Policy focusing on the protection of confidential information, non-disclosure obligations, employee awareness, information handling and responsible use of Company information.
2.0	10 August 2026	Risk Management and Governance Committee	Board of Directors	Revised and expanded into the Company's corporate policy structure under VNG-GOV-CONF-PL-02. Strengthened governance, information classification, need-to-know access, trade secret and personal data protection, third-party confidentiality obligations, incident reporting, KPIs, monitoring, reporting and integration with ERM and relevant internal policies.